

Oppgave 2

Sammenligner de krypterte pakkene fra oppgave 2 med de ukrypterte fra Oppgave 1:

Capturing from Loopback: lo0 (port 5000)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	UDP	38	50276 → 5000 Len=6
2	0.014049	127.0.0.1	127.0.0.1	UDP	72	5000 → 50276 Len=40
3	0.014070	127.0.0.1	127.0.0.1	UDP	42	5000 → 50276 Len=10

Frame 2: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface lo0, id 0

- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- User Datagram Protocol, Src Port: 5000, Dst Port: 50276
- Data (40 bytes)

0000 02 00 00 00 45 00 00 44 2e 0c 00 00 40 11 00 00E..D...@...

0010 7f 00 00 01 7f 00 00 01 13 88 c4 64 00 30 fe 13d..C

0020 48 65 6c 6c 6f 21 20 59 6f 75 72 20 61 72 65 00 Hello! You are

0030 63 6f 6e 6e 65 63 74 65 64 20 74 6f 20 74 68 05 connecte d to the

0040 20 73 65 72 76 65 72 21 server!

Loopback: lo0: <live capture in progress> Packets: 3 · Displayed: 3 (100.0%) Profile: Default

Med kryptering:

src — java -Djavax.net.ssl.keyStore=/Users/sivertutne/mykeystore/examplestore -Djavax.net.ssl.keyStorePassword=password...
sivertutne@Siverts-MacBookPro src % javac SSLServer.java && java -Djavax.net...
.ssl.keyStore=/Users/sivertutne/mykeystore/examplestore -Djavax.net.ssl.keyS...
torePassword=password "SSLServer"
SSL ServerSocket started
[SSL: ServerSocket[addr=0.0.0.0/0.0.0.0,localport=8000]]
ServerSocket accepted
Test
Test
□

src — java -Djavax.net.ssl.trustStore=/Users/sivertutne/mykeystore/examplestore -Djavax.net.ssl.trustStorePassword=password...
sivertutne@Siverts-MacBookPro src % javac SSLClient.java && java -Djavax.net...
.ssl.trustStore=/Users/sivertutne/mykeystore/examplestore -Djavax.net.ssl.tr...
ustStorePassword=password "SSLClient"
Enter something:
Test
Test
Enter something:
Test
Test
Enter something:
□

Capturing from Loopback: lo0 (port 8000)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TLSv1...	90	Application Data
2	0.000062	127.0.0.1	127.0.0.1	TCP	56	8000 → 54987 [ACK] Seq=1 Ac...
3	0.000584	127.0.0.1	127.0.0.1	TLSv1...	90	Application Data
4	0.000624	127.0.0.1	127.0.0.1	TCP	56	54987 → 8000 [ACK] Seq=35 A...

Frame 4: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface lo0, id 0

- Null/Loopback
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
- Transmission Control Protocol, Src Port: 54987, Dst Port: 8000, Seq: 35, Ack: 35, Len: 0

0000 02 00 00 00 45 00 00 34 00 00 40 00 40 06 00 004...@...

0010 7f 00 00 01 7f 00 00 01 d6 cb 1f 40 ce b8 d6 95@...

0020 85 7a 61 f9 80 10 18 cb fe 28 00 00 01 01 08 0a ..za.....{.....

0030 20 92 35 6a 20 92 35 6a ..5j..5j